ELSEVIER

Journal of Retailing xxx (xxx, 2020) xxx–xxx

Journal of Retailing

Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review

Shintaro Okazaki [a,*], Martin Eisend [b], Kirk Plangger [a], Ko de Ruyter [a,d], Dhruv Grewal [c]

[a] *King's Business School, King's College London, Bush House, 30 Aldwych, London WC2B 4BG, UK*
[b] *Center for Market Communications, Europa-Universität Viadrina Frankfurt (Oder), Große Scharrnstraße 59, 15230 Frankfurt (Oder), Germany*
[c] *Marketing Division, 213 Malloy Hall, Babson College, Babson Park, MA 02457, USA*
[d] *UNSW Business School, University of New South Wales, Sydney, New South Wales 2052, Australia*

Abstract

Despite noteworthy advances in theory and retail practice, the extant scholarship on customer privacy concerns is scattered across a wide range of academic domains and remains fragmented, in terms of both conceptual breadth and empirical results. This lack of convergence creates a pertinent need for a comprehensive synthesis to guide to further theory-building and managerial practice with respect to customer concerns about privacy. Unlike earlier meta-analysis studies, this paper reports on a comprehensive meta-analytic review of customer privacy concerns literature, which focuses on strategic retail-relevant variables. Based on 1,103 effects in 304 papers, we offer several key insights that are pertinent to retail scholars and managers who wish to empirically capture and mitigate the impact of customer privacy concerns. We identify two substantive moderators—retail channels and data sensitivity—that wield significant influence in attenuating or strengthening the impact of customer privacy concerns on key retail outcomes. Retail researchers should also consider the significant influences of the research setting, including region, measurement scale, participant selection, and research design. Considering these findings, we conclude the paper by offering a future research agenda that identifies key areas requiring further scrutiny.

Keywords: Customer privacy concerns; Retail channels; Data sensitivity; Research setting; Meta-analysis

Retailers collect and store unprecedented quantities of data from and about their existing and prospective customers to gain insights and improve their offerings and customers' experiences across multiple channels (Plangger and Watson 2015). Many customers willingly share their personal information in exchange for benefits, such as personalized online offers, increased convenience, and location-relevant mobile content (Aguirre et al. 2015; Rainie and Duggan 2016). However, a growing contingent of customers also expresses concerns about their personal privacy (Inman and Nikolova 2017). This can be clearly attributed to infamous malpractice cases, such as Target's microtargeting of pregnant customers (Hill 2012), and high-profile fraud incidents, such as Marriott's $123 million fine for a data breach that exposed the personal data of 383 million customers (Whittaker 2019). These privacy incidents and data breaches are expected to rise (Hodge 2019) and regulators around the world are adopting more stringent interventions, such as the European Union's General Data Protection Regulation. Forward-thinking retailers thus recognize that addressing customer privacy concerns is a strategic imperative. Hence, there is a pertinent managerial need to develop an in-depth understanding of the business impact of customer privacy concerns and mitigation strategies moving forward.

An extensive, multidisciplinary knowledge base on privacy concerns is rapidly evolving and holds the promise of shedding light on the challenges faced by retailers. Researchers have actively studied privacy concerns across a wide array of disciplines, including, notably: marketing, information systems, communication, psychology, sociology, law, and economics. This has resulted in several narrative reviews (Bélanger and Crossler 2011; Smith, Dinev, and Xu 2011); critical reviews (Beke, Eggers, and Verhoef 2018; Martin and Murphy 2017); research agendas (Pavlou 2011); and meta-analytic reviews (Baruh, Secinti, and Cemalcilar 2017; Bauer and Schiffinger

* Corresponding author.
E-mail address: shintaro.okazaki@kcl.ac.uk (S. Okazaki).

https://doi.org/10.1016/j.jretai.2020.05.007

2016; Yun, Lee, and Kim 2014). One drawback of this voluminous body of review-based scholarship is that its relevance to contemporary retailing strategies is unclear. For instance, a recent meta-analysis by Baruh et al. (2017) departs from a broad and generic notion of (not necessarily "customer") privacy concerns, containing sizable study and effect size samples that draw from the general management and communications domains. As a result, the findings and implications are limited in their relevance to retailers.

Our paper adds to the scholarly knowledge base on customer privacy concerns by focusing on key customer outcomes uniquely relevant to retailers, while drawing on evidence from a wide set of academic research domains. Specifically, we explore the differential effects of retail channels and data sensitivity contexts in relation to retail-relevant customer privacy outcomes (see Table 1). Following best meta-analytic practice (Kirca, Jayachandran, and Bearden 2005; Rubera and Kirca 2012), we offer three specific contributions to the retailing literature. In turn, these help us delineate parallel agendas for future research projects and managerial practice in retail.

First, this paper offers much-needed insights into how customer privacy concerns differentially impact customer evaluative and behavioral outcomes across a range of retail channels, since this has direct consequences for the pursuit of multi- and omnichannel strategies by retailers. Recently emerging evidence suggests that retail customers who primarily use mobile or social channels are less concerned about their privacy (Barth and de Jong 2017). At the same time, it is on these platforms that most privacy scandals have occurred (e.g., Facebook, Twitter, WeChat, TikTok). Hence, there is a serious need to examine whether this is influencing the salience of customer privacy concerns in relation to these channels (Aguirre et al. 2015). A key finding of our meta-analytic review is that three retail channels—web, mobile, and social—significantly influence the effects of customers' privacy concerns on their evaluations and behaviors. Specifically, the deployment of social channels increases risk perception, disclosure, and use behaviors; whereas web channels have realized decreases in both risk perception and use behaviors.

Second, this paper investigates how the sensitivity of the data requested by retailers may impact attitudinal and behavioral consequences around customer privacy concerns. It has been argued that data sensitivity is of importance to retailers, due to how intimate the data are and how vulnerable their exposure leaves customers (Inman and Nikolova 2017; Mothersbaugh et al. 2012). Compared to simple demographic data, sensitive data—such as health or financial details—strongly increase customers' perception that their privacy is at risk in retail settings (Anderson and Agarwal 2011; Sheehan and Hoy 2000). To date, however, no meta-analytical studies have explicitly focused on the intensifying risk effect of data sensitivity, despite its potentially significant effect on retail key performance indicators (KPIs). We find that retail contexts involving highly sensitive data decrease customers' perceptions of usefulness and their use behavior, for example.

Third, this paper examines how research setting choices—such as regional contexts, measurement scale,

Table 1
Meta-Analysis of Customer Privacy Concerns.

Study	Main topic	Keywords	Meta-Sample		Substantive factors		Research setting factors			
			Papers	Effect sizes	Retail channel	Data sensitivity	Region	Scale choice	Sample	Research design
Yun et al. (2014)	Online privacy concerns	Privacy concerns, privacy risk, security concerns	89	271	No	No	Yes	Yes	Yes	Yes
Bauer and Schiffinger (2016)	Privacy calculus	Disclosure, self-disclosure, disclose, disclosing	38	148	No	No	No[1]	No	No	No
Wang, Min, and Han (2016)	Risk, privacy concerns, trust	Risk, individual, behavior, social media, trust	43	56	No	No	No[1]	No	No	No
	Online privacy concerns	Privacy concern, privacy knowledge, protective behavior	166	260	No	No	No[1,2]	No	No	No[3]
This study	Retail customers' privacy concerns	Customer privacy concerns, information privacy, privacy concerns, information privacy concerns	310	1,103	Yes	Yes	Yes	Yes	Yes	Yes

Notes: [1] Examines effects of culture; [2] Examines effects of regulatory regime; [3] Examines online versus offline data collection methods.

Please cite this article in press as: Okazaki, Shintaro, et al, Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review, *Journal of Retailing* (xxx, 2020), https://doi.org/10.1016/j.jretai.2020.05.007

sample, and research design—influence the effects of customer privacy concerns on retail KPIs. While these effects appear to be related to the regions in which data are collected, there are conflicting results from past meta-analysis studies (Bauer and Schiffinger 2016; Baruh et al. 2017; Yun et al. 2014). Additionally, there are different scales to measure customer privacy concerns that have different lengths and subdimensions. Yet, apart from a couple of studies (Tully and Winer 2014; Yun et al. 2014), we have little insight into how these choices impact measurement. Researchers also select their research sample and design based on personal preferences, expertise, financial constraints, or other factors—a topic that has been investigated just once, by Yun et al. (2014), prior to this study. Notably, we find significant moderating effects around how customers' privacy concerns impact retail KPIs, according to region, scale choice, sample, and research design.

To arrive at a viable research agenda and actionable guidelines for managerial practice, this paper is structured as follows. First, we discuss retailing research on customer privacy concerns and present our research model. Next, we examine and develop hypotheses regarding the substantive factors of the retail channel and data sensitivity context. We also outline past investigations on the research setting factors of region, measurement scale, research sample, and research design. Last, we describe the meta-analysis sample and method, and interpret and discuss the implications of our findings.

Retailing Research into Customer Privacy Concerns

Customers' privacy concerns stem from a general lack of control over their personal data and/or from doubts about how retailers will handle their data in commercial transactions or communications (Inman and Nikolova 2017; Plangger and Montecchi 2020). Before disclosing their personal data, customers sometimes compare the perceived costs with the benefits promised in exchange, in a cognitive privacy calculus (Culnan and Bies 2003; Lwin, Stanaland, and Miyazaki 2008; Plangger and Montecchi 2020). Customers' privacy concerns become serious obstacles if they perceive the costs to exceed the benefits offered. Thus, prior research details both how these concerns are activated and what methods retailers can use to disrupt this activation.

In their efforts to understand this privacy calculus, scholars consider various contexts, persuasion attempts, and consequences. First, retailing studies note that customer privacy concerns may be specific to web channels (Eastlick, Lotz, and Warrington 2006), personalized online advertising (Bleier and Eisenbeiss 2015); innovative retail technologies (Inman and Nikolova 2017); multichannel retailing (Zhang et al. 2010); and online retailing targeted at children (Lwin et al. 2008). Omnichannel retailers work to deliver offers tailored to customers, yet these can also activate customer privacy concerns (Zhang et al. 2010). Notably, customer privacy concerns are reportedly lower for mobile contexts—compared to location-based advertising or smart shelves—yet relatively higher than for self-checkout scenarios (Inman and Nikolova 2017).

Second, when they are activated by retailers' requests for, or usage of, their personal data (Plangger and Watson 2015), customers' privacy concerns can have negative effects on retail KPIs. Across retail channels, customers are continually exposed to persuasive messages (e.g., ads, salespeople) and from these experiences they learn how to respond to and cope with persuasion attempts (Wright 1986). Customers can observe persuasion efforts by persuasion agents (e.g., retailers, advertisers) and respond with different defensive mechanisms (e.g., customer privacy concerns) that have effects on how they think, feel, and behave (Hardesty, Bearden, and Carlson 2007). For instance, if a retailer collects extremely sensitive personal data, customer privacy concerns may be activated—cueing defensive outcomes, with potentially negative consequences for retailers.

This research focuses on how the outcomes of customer privacy concerns change, with two substantive factors—retail channel and data sensitivity—and with four research setting factors: region, measurement scale, research sample, and research design (see Fig. 1 for our research model). Like other retailing research (e.g., Mathwick, Wagner, and Unni 2010; Orth and Crouch 2014), we specify two main groups of customer outcomes that are relevant to retail practice (i.e., KPIs) and that result from privacy concerns. These are *evaluative* and *behavioral outcomes* (see Table 2). *Evaluative outcomes* are cognitive or affective reactions that result from perceived threats to privacy (e.g., positive evaluations, trust, usefulness perceptions, and risk perceptions). *Behavioral outcomes* are intended or actual actions in response to privacy threats (e.g., disclosure, purchase, use, positive post-use behaviors, and protection behaviors). Based on the support of prior customer privacy concerns research, we hypothesize:

Hypothesis 1. Customers with higher customer privacy concerns exhibit decreased (a) positive evaluation, (b) trust, (c) usefulness; and increased (d) risk.

Hypothesis 2. Customers with higher customer privacy concerns exhibit decreased (a) disclosure, (b) purchase, (c) use, (d) positive post-use behavior; and increased (e) protection behaviors.

Influences of Retail Conditions on Privacy Concerns and their Outcomes

A variety of retail conditions can influence the effect of customer privacy concerns, including the retail channel and data sensitivity. We examine these two substantive factors, as well as exploring the influences of research setting choices (see Table 3). Many of these factors have not served as the primary focus of any specific article. Yet, by using a meta-analysis, we can derive the effect sizes of privacy concerns for different conditions involving these factors. That is, empirical findings related to these moderating factors help reveal the intricate relationships between customer privacy concerns and their outcomes.

Please cite this article in press as: Okazaki, Shintaro, et al, Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review, *Journal of Retailing* (xxx, 2020), https://doi.org/10.1016/j.jretai.2020.05.007

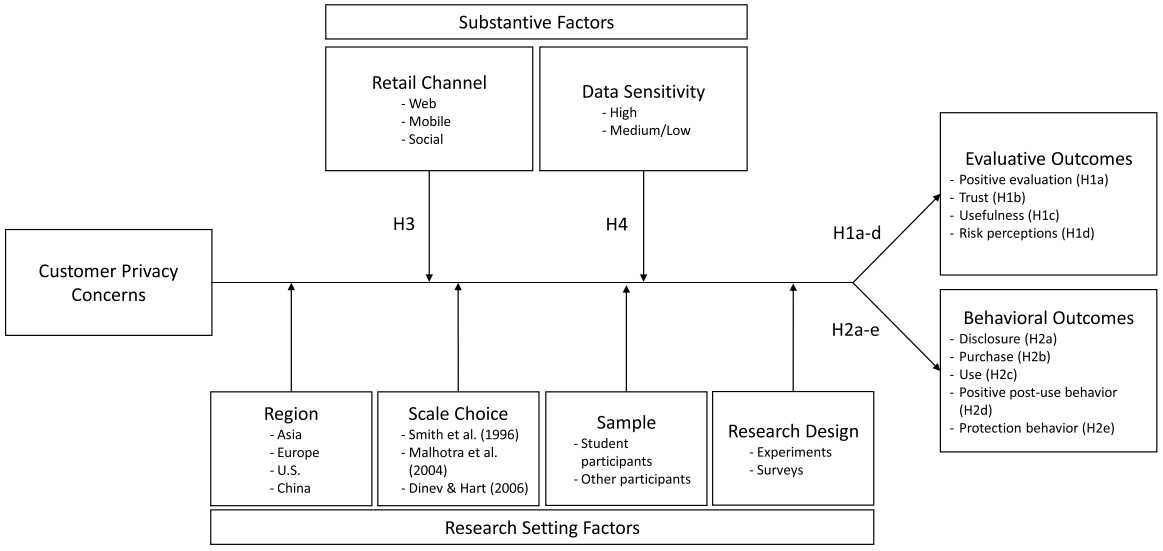

Fig. 1. Research model.

Retail Channels

Customer privacy concerns appear to reflect the technological applications used. Prior research notes the influences of direct marketing, e-commerce, data mining and profiling, monitoring and surveillance, ubiquitous computing, and social media (Smith et al. 2011). Retailers use social channels to regularly communicate with customers by posting useful and engaging content, while simultaneously collecting personal data to improve their personalized marketing strategies. In their review, Barth and de Jong (2017) argue that users of mobile apps or social networks prioritize apparent gains over risks; the irresistible benefits or appeal of these channels appear to compensate perceived threats to privacy. They also note the irrationality of decision making on mobile devices, which often reflects intuition rather than careful assessments of potential privacy risks.

Privacy protection options, such as using junk mail filters or providing fake information to guard against privacy threats, are less available to customers downloading and installing mobile apps, and "the majority of users do not possess the expertise nor the experience to engage in what would be considered appropriate protective behavior" (Barth and de Jong 2017, p.

Table 2
Outcomes of Retail Customers' Privacy Concerns.

Outcome variable	Definition	Sample related variables	Expected relationship
Evaluative outcomes			
Positive evaluation (H1a)	Positive evaluation of a retailer, product, technology, or service	Attitude, enjoyment, attraction, perceived value, performance expectancy	Negative
Trust (H1b)	Trust in a retailer, product, service, or technology	Customer trust, perceived seller trustworthiness, trusting beliefs	Negative
Usefulness (H1c)	Extent of belief that a retailer, product, technology, or service will help perform a task	Perceived usefulness, informativeness, diagnosticity	Negative
Risk (H1d)	Perceived risk and uncertainty regarding consequences of the use of a retailer, product, technology, or service	Perceived risk, financial risk, psychological risk, social risk, risk beliefs, risk perceptions	Positive
Behavioral outcomes			
Disclosure (H2a)	Intention to disclose or disclosure of personal information	Intent to disclose, intention/willingness to give information, disclosure behavior	Negative
Purchase (H2b)	Intention to purchase or actual purchase of a product, technology, or service	Purchase intention, willingness to transact, purchase behavior	Negative
Use (H2c)	Intention to use, reuse, adopt, and usage of a retailer, product, service, or technology	Usage intention, intention to use, intention to adopt	Negative
Positive post-use behavior (H2d)	Positive behaviors after use of a retailer, product, technology, or service	Intention to return, repurchase behavior, continuance intention, patronage intention, recommendation	Negative
Protection behavior (H2e)	Intention or actual behavior to protect from privacy intrusion	Defensive behavior, technical protection, privacy measure use, intention to use firewall, withholding, nondisclosure	Positive

Please cite this article in press as: Okazaki, Shintaro, et al, Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review, *Journal of Retailing* (xxx, 2020), https://doi.org/10.1016/j.jretai.2020.05.007

Table 3
Moderators of Customer Privacy Concerns.

Moderator	Definition or operationalization	Values (sample)
Retail channel (H3)		
Web	Whether the communication/transaction channel is on a website.	1 = web (100 datasets); 0 = other (129 datasets)
Mobile	Whether the communication/transaction channel is using a mobile device.	1 = mobile (47 datasets); 0 = other (182 datasets)
Social	Whether the communication/transaction channel is on social media.	1 = social (82 datasets); 0 = other (147 datasets)
Data sensitivity (H4)	How sensitive are the data for consumers? Data were coded as highly sensitive when they referred to personal data that could be traced back to an individual and result in harm to that person if disclosed—such as biometric data, health data, or financial data.	1 = high (53 datasets); 0 = low/moderate (243 datasets)
Research setting: Region		
Asia	Whether customer privacy concerns are examined in Asian countries (excluding China).	1 = Asia w/o China (56 datasets); 0 = other (240 datasets)
Europe	Whether customer privacy concerns are examined in European countries.	1 = Europe (50 datasets); 0 = other (246 datasets)
USA	Whether customer privacy concerns are examined in the United States.	1 = USA (157 datasets); 0 = other (139 datasets)
China	Whether customer privacy concerns are examined in China.	1 = China (19 datasets); 0 = other (277 datasets)
Research setting: Measurement scale		
Smith et al. (1996)	Whether customer privacy concerns are measured by Smith et al.'s scale.	1 = Smith et al. (347 effect sizes); 0 = other scale (303 effect sizes)
Malhotra et al. (2004)	Whether customer privacy concerns are measured by Malhotra et al.'s scale.	1 = Malhotra et al. (158 effect sizes); 0 = other scale (492 effect sizes)
Dinev and Hart (2006)	Whether customer privacy concerns are measured by Dinev and Hart's scale.	1 = Dinev and Hart (145 effect sizes); 0 = other scale (505 effect sizes)
Research setting: Other method choices		
Experimental design	Whether data are collected with experimental or survey designs.	1 = experiment (31 datasets); 0 = survey (265 datasets)
Student sample	Whether the sample is a student sample.	1 = only students (117 datasets); 0 = other (179 datasets)

Notes: The measurement scale choice variable is measured at the effect size level, and all other variables are measured at the study level. Descriptives for the variables data sensitivity; region (Asia, Europe, USA, and China); experimental design; and student sample are reported for 1,103 effect sizes from 304 papers with 296 datasets. The base alternative for regions is 14 datasets that refer to countries outside of the US, Europe, and Asia (e.g., Australia, Nigeria) or a mix of different countries that could not be assigned to a single region. The channel variables (web, mobile, and social) are reported for 229 datasets, because 67 datasets refer to internet channels in general or a mix of web, mobile, or social channels.
The scale variables (Dinev and Hart 2006; Malhotra et al. 2004; Smith et al. 1996) are reported for 650 effect sizes, because 453 effect sizes refer to the use of any other scale—including those that mix the items from the three scales by Smith et al. (1996), Malhotra et al. (2004), and Dinev and Hart (2006).

1051). For many customers, sharing their personal information on mobile apps represents a routine behavior, yet this disclosure is often perceived as risky (Okazaki, Navarro-Bailón, and Molina-Castillo 2012). In more established retail channels, such as on the web, privacy concerns are inherent determinants of customers' general perceptions of a retail transaction's risk (Pan and Zinkhan 2006). Thus, the perceived privacy risk associated with mobile or social channels appears to be different from that evoked by web channels.

To date, relatively little comparative research has examined differences in privacy concerns among different retail channels. Moreover, the literature lacks a clear understanding of the potential differences and similarities arising from privacy concerns across certain retail channels. Do customer privacy concerns have similar impacts on customer outcomes in mobile and social channels? With the following hypothesis as a foundation, we test for moderating influences of the retail channel context on the evaluative and behavioral outcomes of privacy concerns:

Hypothesis 3. Compared with web channels, mobile or social channels increase the impact of privacy concerns on evaluative and behavioral outcomes.

Data Sensitivity

The type of data requested may influence customers' responses to customer privacy concerns, especially when the data requested are extremely sensitive (Smith et al. 2011). Data sensitivity is dependent on how intimate that data is to the individual, "where greater intimacy is related to information that is perceived as riskier to disclose due to the vulnerability to loss incurred by its disclosure" (Mothersbaugh et al. 2012, p. 77). Individuals may experience exacerbated losses if personal information is more sensitive; thus, the individual is likely to perceive a greater threat (Bansal, Zahedi, and Gefen 2010, 2016). Consider, for example, an insurance company's disclosure request for medical records—compared to their request for an individ-

Please cite this article in press as: Okazaki, Shintaro, et al, Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review, *Journal of Retailing* (xxx, 2020), https://doi.org/10.1016/j.jretai.2020.05.007

ual's gender. Medical records are among the most sensitive data individuals possess (Anderson and Agarwal 2011; Sheehan and Hoy 2000), especially when compared to a simple demographic such as gender. Individuals with high customer privacy concerns are thus likely to show different evaluative and behavioral outcomes, including the intention to disclose, depending on the data sensitivity of the information requested. Formally:

Hypothesis 4. Contexts that contain highly (vs. less) sensitive personal data increase the effects of customer privacy concerns on evaluative and behavioral outcomes.

Research Setting

Although not directly related to privacy concerns, we explore the potential impact of four research setting factors on privacy concerns' effect on customer outcomes. While no formal hypotheses are developed, this exploration may aid future researchers in interpreting their own research findings.

First, customers' privacy concerns tend to vary, along with sociological differences across regions (Plangger and Montecchi 2020; Yun et al. 2014). For example, Bauer's and Schiffinger's (2016) and Baruh, et al.'s (2017) meta-analyses examined the effect of national cultures in terms of Hofstede's cultural dimensions. They found no effect on the role of customer privacy concerns. On the other hand, Yun et al. (2014) study indicates that the correlation of customer privacy concerns with customers' willingness to use online services is significantly stronger in non-U.S. samples, compared with U.S. samples. The authors concluded that individuals in some other countries or regions are generally more concerned about privacy than are those in the U.S. Similarly, other studies (Borena et al. 2015; Lowry, Cao, and Everard 2011) also attributed differences in the effects of customer privacy concerns to national or regional differences. More research is needed to measure the effects of customer privacy concerns in different regions. Yet the literature shows some differential effects of customer privacy concerns on evaluative and behavioral outcomes, depending on the research location (e.g., Asia, Europe, US, China).

Second, researchers' choice of a measurement scale for customer privacy concerns has been found to change the assessed outcomes (Yun et al. 2014). The literature on customer privacy concerns is dominated by three scales: those proposed by Smith et al. (1996); Malhotra et al. (2004); and Dinev and Hart (2006). These scales vary in terms of the length, conceptual dimensions, and research context. Yun et al. (2014) report that scale choice influences the effect sizes of customer privacy concerns on a range of evaluative and behavioral outcomes.

Third, the selection of participants may bias or influence the outcomes around privacy concerns. Specifically, the selection of student versus non-student samples has been shown to have differential effects of customer privacy concerns on outcomes (Yun et al. 2014). These findings suggest that younger student samples will show weaker customer privacy concern effects on evaluative and behavioral outcomes.

Fourth, the researcher's choice of research design (i.e., experiment vs. survey) may impact not just the effect of customer privacy concerns on outcomes, but also the generalizability and validity of their findings (Lee and Baskerville 2003). Experimental designs manipulate and control one or more (predicted) causal variables and observe the differences in outcomes, with the ability to control for confounding variables (Vargas, Duff, and Faber 2017). Survey designs may raise concerns about response rates and nonresponse bias (Peytchev, Baxter, and Carley-Baxter 2009). Thus, according to the degree of control over the confounding variables and biases that result from surveys, the outcomes of customer privacy concerns may differ depending on the choice of research design.

In short, these hypotheses and the discussions underlying them indicate the need for further research into how various potential factors might alter the influence of customer privacy concerns on key evaluative and behavioral outcomes—which, in turn, determine effective retail strategies. To establish a research agenda, we thus undertake a quantitative, meta-analytical synthesis of the current empirical evidence.

Meta-Analysis

A meta-analysis combines results from many studies with similar research questions that produce different, or even conflicting, findings. It represents an effective means to establish a research synthesis and encourage model development (e.g., Eisend 2014; Grewal et al. 2018; Palmatier, Houston, and Hulland 2018). In this section, we detail the sample of papers included in our meta-analysis, our coding procedure, and the analytical approach.

Sample

The sources included all provide estimates of the effects of customer privacy concerns on important customer outcomes, and they span journal articles, working papers, dissertations, and conference proceedings available between 1996 and June 2018. We use this starting year to reflect the appearance of Smith et al. (1996) influential scale, which many privacy researchers identify as a critical milestone (e.g., Li 2011). By including not just published papers but also working papers, dissertations, and conference proceedings, we seek to avoid publication or selection biases (i.e., by minimizing the potential for higher effect sizes in published versus unpublished studies and in articles in peer-reviewed journals) (Eisend and Tarrahi 2014).

To identify these sources, we started with a keyword search of journal articles in electronic databases (ProQuest Research Library, EBSCO, JSTOR, and ScienceDirect), using "information privacy," "privacy concerns," "customer privacy concerns," and "information privacy concerns" as keywords. In addition, we searched digital libraries for conference papers and working papers, and we retrieved doctoral dissertations from ProQuest Dissertations & Theses Global. We also conducted a Google Scholar search to find published papers that might not have entered the databases. Next, we contacted the authors of papers that featured incomplete empirical or methodological information (e.g., missing information about the scales used or variable correlation matrix) and requested this information. Finally, in

Please cite this article in press as: Okazaki, Shintaro, et al, Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review, *Journal of Retailing* (xxx, 2020), https://doi.org/10.1016/j.jretai.2020.05.007

an attempt to include all relevant papers, we cross-checked the references of privacy concern review articles against our own (Baruh et al. 2017; Bauer and Schiffinger 2016; Bélanger and Crossler 2011; Beke et al. 2018; Li 2011; Lowry, Dinev, and Willison 2017; Martin and Murphy 2017; Miltgen and Peyrat-Guillard 2014; Smith et al. 2011; Yun et al. 2014; Zhu and Tao 2015).

Our search efforts yielded 489 papers that contained quantitative empirical data. We dropped eight papers, due to their lack of relevance to the retail context. We excluded papers with insufficient data for effect size calculation and for which the information could not be received from the authors. This left 310 papers for the meta-analysis (see Web Appendix A for a flow chart documenting the retrieval process). The sample thus includes empirical papers that measure customer privacy concerns and identify the correlations between this construct and user responses—as well as research for which the authors responded to our requests for the information needed to compute correlations.

To ensure the independence of our database and avoid duplications, we defined a "paper" to refer to any document that contains the original analysis and findings. Some papers analyzed multiple datasets (e.g., series of experiments), and some datasets were analyzed by more than one paper (e.g., the same dataset and findings were published as conference proceedings and then in a journal article). To avoid duplication, we base our analysis on datasets. The database for the meta-analysis thus comprises 310 papers with 302 datasets, which appeared between 1996 and June 2018. Web Appendix B lists the papers, datasets, and effect sizes.

Coding Procedure

Beyond collecting basic article information (e.g., author, year) and relevant statistics (e.g., correlations, reliabilities, sample sizes), we coded different types of user responses and moderator variables. We identified 1,260 effect sizes in the 302 datasets pertaining to the relationship between customer privacy concerns and any kind of user response. If a particular response variable appeared in just one or two independent datasets or in only one paper—such that we could not build a category with a sufficiently large number of effect sizes (i.e., three or more)—we eliminated it from further analysis. These variables included the perceived quality of coworker, management, or supervisor relationships and social capital. With this step, we ensure a minimum degree of generalizability. The sample was thus reduced to 1,205 effect sizes. Amongst these 1,205 effect sizes are 102 relating to dependent variables that we did not consider relevant in a retailing context; they were thus excluded.[1] The remaining 1,103 effect sizes that we report in the manuscript were taken from 304 papers with 296 datasets.

To ensure consistency in the coding, all studies were coded by one author. For most moderators and for the effect sizes, the coder had to locate the information in the article and transfer it to the database (Cooper 2009). Said information was coded by one author and double-checked by two other authors. The assignment of the dependent variables to the categories, as presented in Table 2, leaves some room for interpretation. They were therefore independently coded by two of the authors. We achieved high coding consistency across the dependent variables, with a kappa value of .911. The coding consistency for moderators, which allowed room for interpretation and were thus coded by two authors, was also high, with kappa values ranging from .853 to .955. Any discrepancies were resolved via discussion.

Analytical Procedure

Integration of Effect Sizes. The effect size metric selected for the meta-analysis was Pearson's correlation coefficient; higher values indicate a stronger influence of customer privacy concerns on outcomes. In addition to the raw effect sizes, we adjusted all correlations for measurement error (Hunter and Schmidt 2004), dividing them by the square root of the product of the reliabilities of the two variables. If a study did not report reliability values or used a single-item measure, we relied on the mean reliability of that construct across all studies.

Before integrating the effect sizes, we addressed potential dependencies among them. If a single dataset established findings for different outcome variables, we treated the findings as independent for our meta-analysis as we analyzed each outcome variable separately. Several datasets provide multiple tests for a given outcome variable. The prior literature offers several options for dealing with this situation, but the preferred procedure to account for dependencies is to deal with the nested error structure. This is both superior to treating the measures as independent and preferable to procedures that represent each dataset with a single value (e.g., average), because it correctly computes the meta-analytic mean and avoids the loss of information and statistical power that occurs when considering only one value from each dataset (Bijmolt and Pieters 2001). We accounted for dependencies in effect sizes and for the nested structure of the meta-analytic data (i.e., multiple effect sizes from one dataset) by using a mixed-effect, multilevel, hierarchical linear model (HLM) to perform the meta-analytic procedures (Raudenbush and Bryk 2002). We consider the variance[2] of each effect size as a weight in this model. The intercept-only model is a random-effects model for meta-analysis.[3]

[1] The mean corrected effect size for the seven dependent variables that were not considered in the subsequent analysis are as follows (with the number of effect sizes in parentheses): Commitment/loyalty (16 ES): $r = -0.222$, $p < 0.05$; Negative evaluation (10 ES): $r = 0.380$, $p < 0.001$; Privacy beliefs (16 ES): $r = -0.321$, $p < 0.001$; Security concerns (12 ES): $r = 0.603$, $p < 0.001$; Satisfaction (19 ES): $r = -0.216$, $p < 0.01$; Regulatory preference (13 ES): $r = 0.355$, $p < 0.05$; Negative post-use behavior (16 ES): $r = 0.168$, $p < 0.05$.

[2] The variance is computed as $V_r = \frac{(1-r^2)^2}{(n-1)}$, with r as the correlation coefficient effect size and n the corresponding sample size.

[3] We estimate the intraclass correlation coefficient ρ for all outcome variables that are used for the moderator analysis. They range between .35 (purchase) and .76 (positive evaluation), indicating that between one-third and more than two-thirds of the observed variance was between studies and that a fair amount of clustering of effect sizes occurred within studies. As such, the use of HLM is appropriate in this context.

Please cite this article in press as: Okazaki, Shintaro, et al, Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review, *Journal of Retailing* (xxx, 2020), https://doi.org/10.1016/j.jretai.2020.05.007

We consider 95% confidence intervals (CIs) around the corrected population correlation point estimates. If the CIs do not include 0, we consider the estimate to be statistically significant at $p < .05$. Another way of looking at the practical relevance of the effect size is via the binomial effect size display (BESD), which illustrates the difference in outcome rates between two groups (here: low and high customer privacy concerns).

With a homogeneity test, we also investigate whether the observed effect sizes vary more than would be expected due to sampling error alone; if they do, it offers a strong rationale to search for moderators. As the homogeneity test, we use the Q statistic, for which the distribution is similar to chi-square with $k - 1$ degrees of freedom, where k is the number of datasets in the meta-analysis (Hedges and Olkin 1985).

We also use fail-safe Ns to check for publication bias (Rosenthal 1979). For a given relationship, the fail-safe N provides an estimate of the number of additional null effects required to render the results for that relationship to the $p = .05$ level. We calculate fail-safe Ns for all significant integrated effect sizes ($p < .05$), using effect size estimates corrected for the study artifacts (i.e., adjusted for measurement error).[4]

Moderator Analysis. If the homogeneity test indicated heterogeneity in the effect size estimates that could not be explained by sampling error alone, we proceeded with a moderator analysis. We first ran a single moderator analysis to test the individual effect of each moderator variable, using HLM. The estimated model for a moderator, measured at the effect size level, is:

$$ES_{ij} = \beta_{0j} + \beta_{1j} * (\text{moderator}_{ij}) + r_{ij}, \text{ with} \quad (1a)$$

$$\beta_{0j} = \gamma_{00} + u_{0j}, \text{ and}$$
$$\beta_{1j} = \gamma_{10}. \quad (1b)$$

The model with a moderator at the dataset level is:

$$ES_{ij} = \beta_{0j} + r_{ij}, \text{ with} \quad (2a)$$

$$\beta_{0j} = \gamma_{00} + \gamma_{01} * (\text{moderator}_{j}) + u_{0j}. \quad (2b)$$

In both models, ES_{ij} is the *i*th effect size, describing the relationship between customer privacy concerns and a particular outcome variable reported in the *j*th dataset. Equation 1a describes the influence of any moderator variables that vary within datasets (i.e., scale types); Eq. (2b) describes the effect of variables that vary across datasets on the intercept, and u_{0j} is the dataset-level residual error term. We did not perform moderator analyses of binary moderators whose values relied on fewer than five effect sizes.

[4] As another test for publication bias, we correlated the effect size (absolute values) with the sample size. If publication bias exists, the sample size should relate negatively to the effect size. This is because small effects from small samples are typically insignificant and should have been excluded if a publication bias existed. The correlation between effect size (absolute values) and sample size in our study was insignificant ($r = -.030$, $p = .294$), thereby indicating that a publication bias was unlikely.

Table 4
Bivariate Correlations of Customer Privacy Concerns with Outcome Variables.

Variables	Data sets	Effect Sizes	Sample Size	Mean *r (Raw)*	Mean *r (Corrected)*	95% CI Lower	95% CI Upper	Homogeneity Test Q	Fail-Safe N
Evaluative Outcomes									
Positive evaluation (H1a)	55	121	23,311	−0.140***	−0.165***	−0.250	−0.097	21457.968***	64,651
Trust (H1b)	60	127	26,630	−0.173***	−0.199***	−0.270	−0.127	9211.953***	89,099
Usefulness (H1c)	17	37	8,265	−0.037	−0.037	−0.177	0.102	1512.314***	–
Risk perceptions (H1d)	65	155	28,330	0.369***	0.429***	0.373	0.485	28062.718***	1,081,936
Behavioral Outcomes									
Disclosure (H2a)	89	197	44,848	−0.185***	−0.211***	−0.248	−0.174	2981.300***	42,303
Purchase (H2b)	44	87	16,927	−0.170***	−0.189***	−0.260	−0.118	2389.598***	10,736
Use (H2c)	106	200	38,723	−0.152***	−0.173***	−0.220	−0.126	9871.523***	114,503
Positive post-use behavior (H2d)	19	26	8,992	−0.194***	−0.221***	−0.310	−0.132	382.3693***	2,502
Protection behavior (H2e)	64	153	28,438	0.245***	0.292***	0.230	0.354	10217.053***	292,136

Note: CI = confidence interval.
*** $p < .001$ (two-tailed tests).

Please cite this article in press as: Okazaki, Shintaro, et al, Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review, *Journal of Retailing* (xxx, 2020), https://doi.org/10.1016/j.jretai.2020.05.007

Table 5
Moderator Analysis.

Moderators	Positive Evaluation	Risk	Trust	Useful-ness	Disclo-sure	Protection	Purchase	Use	Positive post-use
Retail channel (H3)									
Web	−0.096 (0.104)	−0.125^{+} (0.065)	0.035 (0.085)	−0.115 (0.189)	−0.031 (0.041)	0.098 (0.073)	0.020 (0.102)	−0.167* (0.067)	–
Mobile	0.084 (0.102)	0.068 (0.064)	−0.139^{+} (0.077)	−0.107 (0.208)	−0.090 (0.054)	−0.138* (0.068)	0.017 (0.122)	−0.036 (0.053)	−0.055 (0.115)
Social	0.045 (0.123)	0.091* (0.049)	0.091 (0.090)	–	0.077^{+} (0.041)	−0.064 (0.074)	–	0.164** (0.051)	0.122 (0.122)
Data sensitivity (H4)									
	−0.101 (0.079)	0.048 (0.052)	−0.100 (0.080)	−0.343^{+} (0.163)	−0.036 (0.049)	–	–	−0.118* (0.057)	−0.005 (0.093)
Research Setting: Region									
Asia	0.195^{+} (0.098)	0.146* (0.065)	−0.025 (0.103)	0.016 (0.149)	0.112* (0.056)	0.046 (0.103)	0.040 (0.088)	−0.005 (0.060)	−0.161 (0.107)
Europe	−0.131 (0.106)	−0.029 (0.062)	0.146^{+} (0.075)	–	−0.081 (0.065)	−0.058 (0.045)	−0.160 (0.139)	0.005 (0.087)	0.075 (0.095)
USA	−0.050 (0.088)	−0.081 (0.055)	0.002 (0.076)	0.068 (0.131)	0.007 (0.043)	−0.081 (0.064)	−0.050 (0.074)	0.009 (0.046)	0.038 (0.094)
China	−0.030 (0.150)	0.144* (0.062)	−0.217* (0.095)	–	–	–	–	0.003 (0.074)	–
Research setting: Measurement scale									
Smith et al. (1996)	0.001 (0.042)	0.077*** (0.020)	0.020 (0.019)	–	−0.046* (0.020)	0.298** (0.108)	−0.011 (0.058)	−0.078 (0.105)	–
Malhotra et al. (2004)	0.069^{+} (0.037)	−0.080*** (0.020)	−0.025 (0.017)	–	0.059* (0.022)	−0.351* (0.136)	0.115^{+} (0.062)	0.056 (0.051)	–
Dinev and Hart (2006)	−0.237* (0.108)	0.024 (0.069)	0.037 (0.067)	–	−0.010 (0.053)	−0.085 (0.126)	−0.274** (0.082)	0.056 (0.107)	–
Smith et al. (1996) × Data sensitivity	0.187 (0.320)	−0.195 (0.118)	−0.200 (0.196)	–	−0.184 (0.121)	–	–	−0.404* (0.099)	–
Malhotra et al. (2004) × Data sensitivity	–	0.275** (0.111)	–	–	−0.039 (0.112)	–	–	–	–
Dinev and Hart (2006) × Data sensitivity	–	–	0.110 (0.162)	–	0.199^{+} (0.115)	–	–	–	–
Research setting: Other method choices									
Experiment design	−0.061 (0.164)	−0.098 (0.107)	−0.115^{+} (0.066)	–	−0.083 (0.050)	−0.032 (0.149)	−0.048 (0.093)	−0.126* (0.052)	–
Student sample	−0.011 (0.083)	−0.171** (0.059)	0.159^{+} (0.083)	−0.036 (0.164)	−0.086 (0.053)	0.032 (0.064)	0.193** (0.067)	0.112* (0.049)	0.130 (0.096)

Notes: Unstandardized regression coefficients and standard errors are in brackets. We did not perform a moderator analysis if the value of a binary moderator was based on fewer than five effect sizes or three studies (indicated by –).

$^{+}$ $p < .10$.
* $p < .05$.
** $p < .01$.
*** $p < .001$.

Please cite this article in press as: Okazaki, Shintaro, et al, Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review, *Journal of Retailing* (xxx, 2020), https://doi.org/10.1016/j.jretai.2020.05.007

Results

The results in Table 4 show—in line with Hypothesis 1a-d—that customer privacy concerns significantly affect evaluative outcomes in the form of decreased positive evaluations and trust, as well as increased risk perceptions. In the only exception to our predictions, customer privacy concerns do not significantly affect usefulness perceptions. As predicted in Hypothesis 2a–e, customer privacy concerns also significantly affect behavioral outcomes. Specifically, they decrease disclosure, purchase, use, and positive post-use behavior but increase protection. A correlation of .292 between customer privacy concerns and protection behavior corresponds to a BESD of ca. 29%. If half of this figure is added and subtracted from 50% (i.e., the base rate if there is no relationship between both variables), the figures indicate that between low and high privacy concerned customers, the likelihood of protection behavior shifts from 35.5% to 64.5%. The effects are also heterogeneous, so moderations are likely. For the significant relationships, the fail-safe *N* values all exceed Rosenthal's (1979) threshold (5 times the number of datasets plus 10), indicating that publication bias is unlikely.

We test each moderating factor—individually and, in some select cases, together—to understand their isolated or interaction effects (see Table 5). These analyses reveal some significant differences in the impact of customer privacy concerns on outcomes.

For Hypothesis 3 (retail channels), the results exhibit some significant moderating influences on customer privacy concerns' effects on outcomes. Compared to other channels, web channels show more negative effects on use behaviors ($r_{web} = -0.302$; $r_{other} = -0.135$)[5] and weaker effects on risk perceptions ($r_{web} = 0.357$; $r_{other} = 0.482$). Mobile channels produce more negative effects on trust ($r_{mobile} = -0.306$; $r_{other} = -0.167$) and smaller effects on protection behaviors ($r_{mobile} = 0.161$; $r_{other} = 0.299$). Social channel studies reveal increased privacy concern effects on risk ($r_{social} = 0.502$; $r_{other} = 0.411$) and fewer negative effects on disclosure ($r_{social} = -0.168$; $r_{other} = -0.245$) and use behaviors ($r_{social} = -0.082$; $r_{other} = -0.245$).

In Hypothesis 4 (data sensitivity), when studies involve highly sensitive data, the results only indicate significantly greater negative effects of customer privacy concerns when it comes to usefulness perceptions ($r_{low/medium} = 0.055$; $r_{high} = -0.288$) and use behaviors ($r_{low/medium} = -0.143$; $r_{high} = -0.262$).

We find many significant effects around research setting. Regarding regional factors, the results show some significant moderating effects. Studies employing Asian samples (without China) report fewer negative effects of customer privacy concerns on positive evaluations ($r_{Asia} = -0.007$; $r_{other} = -0.203$) and disclosure ($r_{Asia} = -0.116$; $r_{other} = -0.228$), but stronger effects on risk perceptions ($r_{Asia} = 0.552$; $r_{other} = 0.406$). When studies rely on Chinese samples, the results show significantly stronger effects of customer privacy concerns on risk perceptions ($r_{China} = 0.555$; $r_{other} = 0.411$), but more negative effects on trust ($r_{China} = -0.393$; $r_{other} = -0.177$).

In terms of measurement scale choice, we note that studies employing Smith et al.'s (1996) scale report more negative effects on disclosure ($r_{Smith} = -0.304$; $r_{other} = -0.258$), but stronger effects on protection behaviors ($r_{Smith} = 0.514$; $r_{other} = 0.216$) and risk perceptions ($r_{Smith} = 0.477$; $r_{other} = 0.400$). Those adopting Malhotra et al.'s (2004) scale identify fewer negative effects on disclosure ($r_{Malhotra} = -0.228$; $r_{other} = -0.287$), use behaviors ($r_{Malhotra} = -0.056$; $r_{other} = -0.171$), and positive evaluations ($r_{Malhotra} = -0.052$; $r_{other} = -0.121$); and weaker effects on risk ($r_{Malhotra} = 0.375$; $r_{other} = 0.455$) and protection behavior ($r_{Malhotra} = 0.029$; $r_{other} = 0.388$). Studies utilizing Dinev and Hart's (2006) scale cite more negative effects of customer privacy concerns on positive evaluations ($r_{Dinev} = -0.294$; $r_{other} = -0.057$) and purchase ($r_{Dinev} = -0.356$; $r_{other} = -0.082$). Combining these insights, we also find significant interaction effects between data sensitivity and scale choice. Studies employing Malhotra et al.'s (2004) scale reveal increased risk perceptions in high sensitivity contexts, relative to low to moderate sensitivity contexts (see Fig. 2). Those employing Smith et al.'s (1996) scale reveal less negative effects on use in low to moderate sensitivity contexts.

We also find significant effects for sample selection and research design. Student samples significantly lead to less negative effects of customer privacy concerns on purchase ($r_{student} = -0.063$; $r_{other} = -0.256$), use ($r_{student} = -0.104$; $r_{other} = -0.215$), and trust ($r_{student} = -0.092$; $r_{other} = -0.252$), but they reduce the effects on risk perceptions ($r_{student} = 0.315$; $r_{other} = 0.486$). Compared to surveys, experimental designs lead to significantly more negative effects of customer privacy concerns on use behaviors ($r_{surveys} = -0.156$; $r_{experiment} = -0.283$) and trust ($r_{surveys} = -0.191$; $r_{experiment} = -0.306$).

Discussion

Theoretical Implications

Our findings have several theoretical implications. First, concerning the direct effects, our results reveal that higher customer privacy concerns significantly decrease positive evaluation (H1a), trust (H1b), disclosure (H2a), purchase (H2b), use (H2c), and positive post-use behaviors (H2d), while significantly increasing risk perceptions (H1c) and protection behaviors (H2e). These findings are consistent with prior literature (Bélanger and Crossler 2011; Inman and Nikolova 2017; Lwin, Stanaland, and Miyazaki 2008) and other privacy concern meta-analyses (Baruh, Secinti, and Cemalcilar 2017; Bauer and Schiffinger 2016; Wang et al. 2016; Yun et al. 2014). While we find no direct relationship between customer privacy concerns and usefulness perceptions (H1c), we call for continued research into this effect since our analysis was limited by the availability of only 17 datasets and 37 effect sizes. Generally, our baseline results on the impact of customer privacy concerns on critical outcome variables may serve as empirical benchmarks for fur-

[5] The values in parentheses are predicted mean effect size values for the subgroups of the dummy variables. For the dummy variable coding, please also see Table 3.

Please cite this article in press as: Okazaki, Shintaro, et al, Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review, *Journal of Retailing* (xxx, 2020), https://doi.org/10.1016/j.jretai.2020.05.007

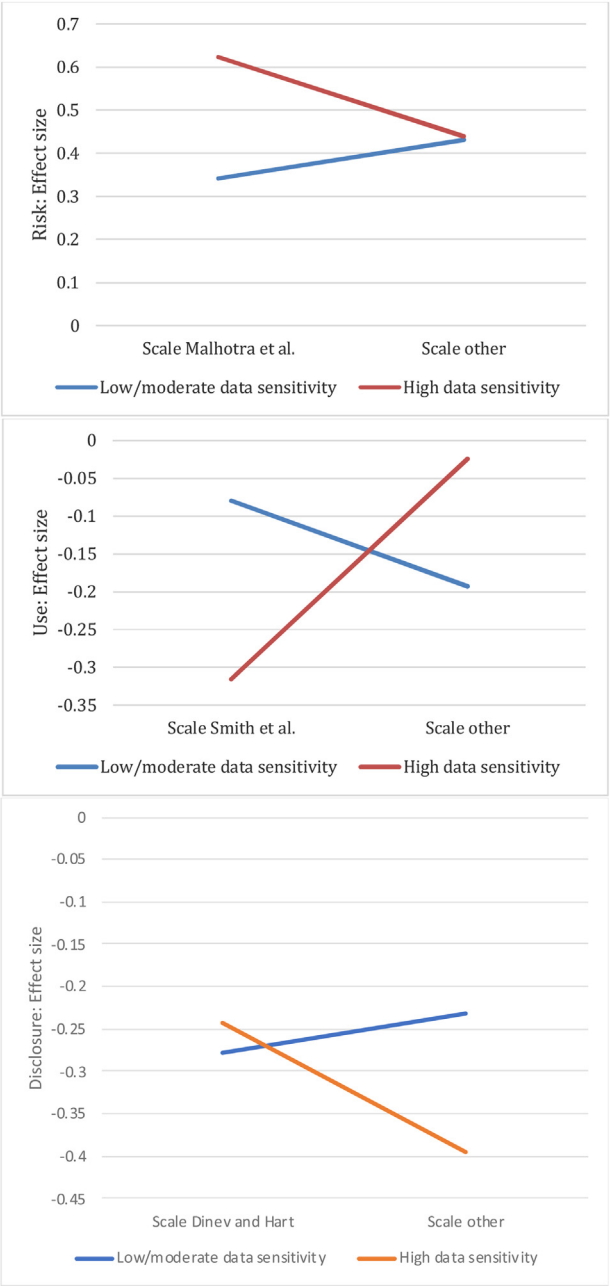

Fig. 2. Interactions of measurement scale choice and data sensitivity context.

ther studies on the role of customer concerns in the retailing context.

Second, our findings indicate that retail channels do significantly and differentially influence the effects of customer privacy concerns, partly confirming our hypothesis (H3). We find that studies using web channels significantly decrease the effects of customer privacy concerns on use behaviors and risk perceptions. Mobile studies report significantly less trust and protection behaviors. However, when people express high customer privacy concerns, social channel studies appear to increase disclosure, use behaviors, and risk perceptions compared to non-social channels. This worrisome finding could partly explain the substantial increase in cyberbullying and on the disclosure of unconsented information on social channels (Weber, Ziegele, and Schnauber 2013). Researchers could use these results to explain the effects of customer privacy concerns in less-established retail channels, and in designing studies to investigate customer privacy concerns in omni- or multichannel retail contexts.

Third, our findings indicate partial support for our hypothesis (H4) that higher data sensitivity will increase privacy concerns' effects. While, indeed, the effects of customer privacy concerns significantly decrease usefulness perceptions and use behaviors, there are either no (i.e., the topic has not received enough research attention) or non-significant results for the remaining consumer outcomes. Thus, while there is a strong theoretical and logical basis around the influence of data sensitivity on the outcomes of customer privacy concerns (e.g., Mothersbaugh et al. 2012)—we cannot conclusively report this effect, except for usefulness and use behaviors. We thus call for more attention to be brought to this area, to clarify these relationships.

Fourth, we find significant effects for all research setting factors. Our region findings indicate significant increases in positive evaluation (Asia without China) risk perceptions (Asia without China, China); trust (Europe); and disclosure (Asia without China), as well as a significant decrease in trust (China). Some of these findings confirm existing research (e.g., the increase in risk perceptions and decrease in trust outside of the USA) (Yun et al. 2014). Yet the relationships among other findings are surprising. Further research is required, to substantiate these effects and better understand their mechanisms, including the roles of cultural, regulatory, and economic development factors. While we performed a post hoc analysis—with GDP per capita as a country variable—and reported no significant findings, we cannot be certain since there still are relatively few studies outside of the USA. This indicates the need for regional diversity in the customer privacy concerns literature, specifically related to the retail context.

As expected, the choice of the scale used to measure customer privacy concerns significantly impacts the outcomes. This confirms Yun et al's. (2014) findings. Researchers must carefully reflect on their scale choice and acknowledge its potential influence, to contextualize their findings. We also find interaction effects between measurement scale choice and data sensitivity, which influence perceived risk and use behaviors. These interaction results muddy the previously detailed moderation results, but the reason for the discrepancies seems to lie in the different scale dimensions. For example, Smith et al.'s (1996) scale consists of collection, errors, unauthorized secondary use, and improper access—while Malhotra et al.'s (2004) scale includes collection, control, and awareness. More research is needed, regarding measurement scale choice and data sensitivity around customer privacy concerns, to understand the significance of these significant interactions.

Moving on to other research setting influences, sample and research design have significant impacts on the effects of customer privacy concerns. For example, customer privacy concerns evoke lower risk perceptions—but higher trust, purchase, and use behaviors—among student samples. Experimental designs significantly decrease customer privacy concerns' effect

Please cite this article in press as: Okazaki, Shintaro, et al, Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review, *Journal of Retailing* (xxx, 2020), https://doi.org/10.1016/j.jretai.2020.05.007

Table 6
Future Directions for Retail Channels.

Retail Marketing Mix	Retail Practice Guidelines	Related Questions for Future Retail Research
Product/brands	Customer data-based recommendations are a key to future growth but need to look at the potential issues related to the data source afforded by the retail channels.	• How can loyalty data be used to promote products based on past transactions, to minimize the activation of customer privacy concerns? • How should retailers present digital behavioral tracking data-based recommendations, to decrease customer perceptions of creepiness? • To what extent should retailers engage in customer data acquisition from social or mobile channels, to improve the effectiveness of artificial intelligence-based product suggestions?
Customer service	When adopting omni- or multichannel strategies, retailers should be mindful of the differential channel effects on customer privacy concerns to provide consistent customer service.	• To what extent should retailers provide different or consistent levels of customer service, depending on the channel? • How can cross-channel loyalty programs help retailers enhance the quality of customer relationships?
Communication	Effectively integrated retail communication strategies ensure consistency of promotional messages but may require tailored tactics based on retail channel characteristics to mitigate customer privacy concerns.	• What communication practices are most appropriate to reduce customer privacy concerns, when communicating with customers across different channels? • Which retail channel-specific strategies are most effective in mitigating customer privacy concerns, while achieving promotional goals? • How can retailers leverage contextual data (e.g., geo-location) to achieve sales goals, without increasing negative consumer reactions?
Incentives/prices	Retailers should modify and leverage pricing and incentive strategies for offline and online retail transactions to increase customers' perceived value.	• What is the most appropriate payment method for each retail channel to reduce customer privacy concerns? • How can retailers maximize the perceived value of monetary and non-monetary incentives in each retail channel, to balance customer privacy concerns? • How do consumer outcomes (e.g., customer satisfaction, loyalty, and word-of-mouth) change when charging more on retail channels that offer additional privacy?
Distribution	Omni-channel and multichannel strategies present unique challenges for retailers, as they both face increasing competition and the need to manage customer privacy concerns.	• When distributing through a new channel, how can retailers gain customer data while protecting customers' privacy? • How can retailers manage customer privacy preferences when implementing an omni-channel strategy? • To what extent do retail channels act as buffers to perceived privacy risks?

on trust and use behaviors, compared with survey designs. Furthermore, technological and social environments have changed dramatically over the more than 22-year period covered. A post hoc analysis to assess the influence of the year of data collection reveals one significant result: the effect of customer privacy concerns on use behaviors increases in newer studies ($b = 0.010$, SE = 0.006, $t = 1.713$, $p = 0.090$). Thus, researchers need to reflect on how their research setting choices and environment can potentially bias their results.

Managerial Implications

As our results confirm, retailers whose customers have high levels of customer privacy concerns will likely face weaker purchase likelihoods, usage rates, information disclosures, consumer trust, positive evaluations, and positive post-use behaviors—as well as increased risk perceptions and displays of protective behaviors. To reduce these adversary effects, proactive retailers must strategize and plan how to alleviate customer privacy concerns. One approach could be to develop new, or add to existing, goodwill strategies—such as philanthropic activities or corporate social responsibility—and enhance retailers' image and reputation by promoting them on mass and social media outlets (Okazaki et al. 2020). Another approach is to develop innovative products and services that either protect customer information or use less of such information beyond what is legally necessary. Apple Inc. and Privacy.com, for example, offer credit "cards" that restrict the sharing or use of their customers' transaction data (Fowler 2019). While there are evident threats posed by customers with high customer privacy concerns, an increased awareness of these concerns among retailers could reduce their risk while also taking advantage of opportunities presented by protecting their customers' privacy.

Our findings also indicate that the specific nature of various retail channels changes the effect of customer privacy concerns on outcomes. Web channels show decreased effects on positive

Please cite this article in press as: Okazaki, Shintaro, et al, Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review, *Journal of Retailing* (xxx, 2020), https://doi.org/10.1016/j.jretai.2020.05.007

Table 7
Future Directions for Data Sensitivity.

Retail Marketing Mix	Retail Practice Guidelines	Related Questions for Future Retail Research
Product/brands	Retailers should develop innovative privacy-augmented products (e.g., store credit cards that do not track transactions) to protect customers' data, especially in highly sensitive contexts.	• How can retail product selections be tailored to mitigate the activation of customer privacy concerns? • When products collect customer data, what product innovations could be introduced to provide customer data security? • To target customers with high customer privacy concerns, how could products be augmented to protect their privacy?
Customer service	While customer service requires customer data to be more effective, retailers in highly sensitive contexts (e.g., pharmacy, banks) should implement privacy and data protecting technologies.	• When transactions necessitate dealing with highly sensitive customer data, what privacy protecting technologies or strategies can be employed to maintain customer satisfaction and loyalty? • What is the best way to provide outstanding customer service that requires customer data, while minimizing customers' risk perceptions?
Communication	Retailers should minimize the use of sensitive customer data from communications and plan for potential data breaches to protect corporate reputation.	• How do retailers offer personalized communication, while minimizing customer data use and without impacting customer satisfaction? • What promotional strategies should retailers use, when collecting or acquiring sensitive customer data? How should retailers differentiate these strategies between web, mobile, and social channels? • Within highly sensitive contexts, what corporate governance strategies could mitigate the reputation fallout of a data breach?
Incentives/price	Pricing or incentive policies should be tailored when highly sensitive data are required, to avoid harming customer value.	• To what extent will customers pay extra for enhanced privacy in different data sensitivity contexts? • When they require sensitive data, how could retailers avoid increasing risk perception while amplifying customer value?
Distribution	To protect highly sensitive data, retailers should be aware of channel-specific privacy risks.	• When dealing with highly sensitive data, which retail channel should customers be directed to, so that their privacy and data are protected? • How can retailers identify the level of potential data or privacy risk in each channel?

evaluation and use behaviors, while mobile channels decrease trust and protection behaviors. Transactions on social channels, on the other hand, show increased risk perception, disclosure, and use behaviors. Retailers using social channels must thus be aware of these effects—and they must also move beyond mere awareness to strategically acquire, store, and destroy customers' data to protect their image and reputation (Plangger and Watson 2015). As major occurrences of personal data theft increase—such as the recent Facebook incident, in which 50 million accounts were exposed (Rosen 2018)—customer privacy concerns in general are likely to increase into the future. So are risk perceptions related to retail transactions via social channels. Retailers that collect customers' personal data are obliged to prepare for unexpected, large-scale data security failures by creating safeguards to protect and ensure information privacy. And, as in so many other instances, retailers are advised to not only "be good, but also tell it." In other words, it is vital to design and carry out communications campaigns that convey the transparent policies that are put into place.

As an increasing number of retailers go global through digital retail channels, these retail managers should reflect on how their global customers' privacy concerns may be influenced by regional factors that differ from where they live. For example, the international airline British Airways was ultimately fined £183 million by European regulators, for a data breach that exposed 380,000 customers' details to hackers (Cellan-Jones 2019). Yet the data breach may have had different effects on consumers, depending on where they lived. Global retailers need to look beyond their local surroundings and consider how other national or regional factors may influence the effects of customers' privacy concerns on retail KPIs—not to mention the firms' reputations—in the effort to plan for and potentially mitigate customer data security incidents.

Limitations and Conclusions

As with all empirical studies, we acknowledge specific limitations of our study. In turn—and in addition to our findings—these can be used to spur further research into customer privacy concerns. First, despite our rigorous search of the relevant articles and repeated requests to authors to provide additional study information, our meta-analysis sample contained only those studies that provided enough statistical information to run our tests. As a result, there may be additional studies that are not

Please cite this article in press as: Okazaki, Shintaro, et al, Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review, *Journal of Retailing* (xxx, 2020), https://doi.org/10.1016/j.jretai.2020.05.007

in our sample that could have led to significant findings for reported (i.e., usefulness perceptions) and unreported (e.g., satisfaction; see footnote 1) outcome variables. Researchers across the globe should be vigilant about the exclusion of papers, in future research—and should, where possible, be inclusive of ideas and suggestions put forward by studies that do not methodologically qualify for inclusion in meta-analytic reviews. Second, we restricted our sample to studies written in English. It is possible that including non-English studies would have influenced our estimates. Again, as the retail research marketplace of ideas is becoming increasingly global, future research should be open to pursuing research opportunities emanating from studies in a variety of languages. Third, while some of the effect size calculations (e.g., usefulness perceptions) rely on a relatively modest number of effects, few studies featured those variables. We thus decided to include these results because of their theoretical interest and practical importance, even though we report weak or non-significant effects. Although we strongly believe that it is important to consider these under-researched outcome variables, our findings were likely influenced by the lack of research in these areas. We suggest that researchers consider these variables to enlarge the realm of potential outcome variables in research designs.

While the customer privacy concerns literature has yielded many insights on main effects, the next generation of retail privacy research must explore, measure, and theorize around additional substantive and contextual factors. This meta-analysis has focused on two important substantive factors: retail channel and data sensitivity. Based on our findings, we suggest retail practice guidelines and future questions for retail research into the elements of the retail marketing mix (see Tables 6 and 7).

As both retailers' customer channels and customers' own preferences become more complex and intricate, it is imperative that retailers remain aware of customer privacy concerns on an ongoing basis. As Steve Jobs argued, *I believe people are smart. Some people want to share more than other people do. Ask them.* When it comes to customer privacy concerns, the continuing challenge for researchers and editors is to assist retailers in framing the questions, and for meta-analysts to review whether these are the "right" questions.

Declarations of interest

None.

Acknowledgement

The authors wholeheartedly thank the three anonymous reviewers and the Guest Editors, Robert Palmatier and Kelly Martin, for their many constructive and helpful comments that greatly improved the final version of this manuscript. We also thank Elisa Schweiger for her valuable feedback on an earlier version of the manuscript. We are also grateful for Victoria Andrade for her support in data collection.

Appendix A. Supplementary data

Supplementary data associated with this article can be found, in the online version, at https://doi.org/10.1016/j.jretai.2020.05.007.

References

Aguirre, Elizabeth, Dominik Mahr, Dhruv Grewal, Ko de Ruyter and Martin Wetzels (2015), "Unraveling the personalization paradox: The Effect of information collection and trust-building strategies on online advertisement effectiveness," *Journal of Retailing,* 91 (1), 34–49.

Anderson, Catherine L. and Ritu Agarwal (2011), "The Digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information," *Information Systems Research,* 22 (3), 469–90.

Bansal, Gaurav, Fatemeh Mariam Zahedi and David Gefen (2010), "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems,* 49 (2), 138–50.

Bansal, Gaurav, Fatemeh Mariam Zahedi and David Gefen (2016), "Do context and personality matter? Trust and privacy concerns in disclosing private information online," *Information and Management,* 53 (1), 1–21.

Barth, Susanne and Menno D.T. de Jong (2017), "The Privacy paradox—investigating discrepancies between expressed privacy concerns and actual online behavior—a systematic literature review," *Telematics and Informatics,* 34 (7), 1038–58.

Baruh, Lemi, Ekin Secinti and Zeynep Cemalcilar (2017), "Online privacy concerns and privacy management: A meta-analytical review," *Journal of Communication,* 67 (1), 26–53.

Bauer, Christine and Michael Schiffinger (2016), "Perceived risks and benefits of online self-disclosure: Affected by culture? A meta-analysis of cultural differences as moderators of privacy calculus in person-to-crowd settings," in *Proceedings of the 24th European Conference on Information Systems (ECIS 2016).*,

Beke, Frank T., Felix Eggers and Peter C. Verhoef (2018), "Consumer Informational Privacy: Current Knowledge and Research Directions," *Foundations and Trends® in Marketing,* 11 (1), 1–71.

Bélanger, France and Robert E. Crossler (2011), "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly,* 35 (4), 1017–41.

Bijmolt, Tammo H. and Rik G. Pieters (2001), "Meta-analysis in marketing when studies contain multiple measurements," *Marketing Letters,* 12 (2), 157–69.

Bleier, Alexander and Maik Eisenbeiss (2015), "The importance of trust for personalized online advertising," *Journal of Retailing,* 91 (3), 390–409.

Borena, Berhanu, France Belanger, E. Dejene and D. Dedefa (2015), "Information Privacy Protection Practices in Africa: A Review through the Lens of Critical Social Theory," *Proceedings of the Annual Hawaii International Conference on System Sciences,*, 3490–7.

Cellan-Jones, Rory (2019), *British Airways faces record £183m fine for data breach,* BBBC News. July 9, available online at: https://www.bbc.com/news/business-48905907 [retrieved on March 35, 2020]

Cooper, Harris (2009), "Hypotheses and problems in research synthesis," in *in The Handbook of Research Synthesis and Meta-Analysis*, Cooper H., Hedges L. V. and Valentine J. C., eds. New York: Russell Sage Foundation, 19–36.

Culnan, Mary J. and Robert J. Bies (2003), "Consumer privacy: Balancing economic and justice considerations," *Journal of Social Issues,* 59 (2), 323–42.

Dinev, Tamary and Paul Hart (2006), "An Extended privacy calculus model for e-commerce transactions," *Information Systems Research,* 17 (1), 61–80.

Eastlick, Mary A., Sherry L. Lotz and Patricia Warrington (2006), "Understanding online b-to-c relationships: An Integrated model of privacy concerns, trust, and commitment," *Journal of Business Research,* 59 (8), 877–86.

Eisend, Martin (2014), "Shelf space elasticity: A Meta-analysis," *Journal of Retailing,* 90 (2), 168–81.

Please cite this article in press as: Okazaki, Shintaro, et al, Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review, *Journal of Retailing* (xxx, 2020), https://doi.org/10.1016/j.jretai.2020.05.007

Eisend, Martin and Farid Tarrahi (2014), "Meta-analysis selection bias in marketing research," *International Journal of Research in Marketing,* 31 (3), 317–26.

Fowler, Geoffrey (2019), *The Spy in your wallet: Credit cards have a privacy problem,* The Washington Post. August 26, available online: https://www.washingtonpost.com/technology/2019/08/26/spy-your-wallet-credit-cards-have-privacy-problem/ [Accessed January 31, 2020]

Grewal, Dhruv, Nancy M. Puccinelli and Kent B. Monroe (2018), "Meta-Analysis: Integrating Accumulating Knowledge," *Journal of the Academy of Marketing Science,* 46 (1), 9–30.

Hardesty, David M., William O. Bearden and Jay P. Carlson (2007), "Persuasion knowledge and consumer reactions to pricing tactics," *Journal of Retailing,* 83 (2), 199–210.

Hedges, Larry V. and Ingram Olkin (1985), *Statistical Methods for Meta-Analysis,* Orlando, FL: Academic Press.

Hill, Kashmir (2012), *How Target figured out a teen girl was pregnant before her father did,* Forbes available online: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/ [Accessed January 21, 2020]

Hodge, R. (2019), *2019 Data breaches hall of shame: These were the biggest data breaches of the year,* CNET available online: https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/ [Accessed January 5, 2020]

Hunter, John E. and Frank L. Schmidt (2004), *Methods of Meta-Analysis: Correcting Error and Bias in Research Findings,* Thousand Oaks, CA: Sage Publications.

Inman, Jeffrey J. and Hristina Nikolova (2017), "Shopper-facing retail technology: A Retailer adoption decision framework incorporating shopper attitudes and privacy concerns," *Journal of Retailing,* 93 (1), 7–28.

Kirca, Ahmet H., Satish Jayachandran and William O. Bearden (2005), "Market orientation: A meta-analytic review and assessment of its antecedents and impact on performance," *Journal of Marketing,* 69 (2), 24–41.

Lee, Allen S. and Richard L. Baskerville (2003), "Generalizing generalizability in information systems research," *Information Systems Research,* 14 (3), 221–43.

Li, Yuan (2011), "Empirical studies on online information privacy concerns: Literature review and an integrative framework," *CAIS,* 28 (1), 453–96.

Lowry, Paul Benjamin, Jinwei Cao and Andrea Everard (2011), "Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures," *Journal of Management Information Systems,* 27 (4), 163–200.

Lowry, Paul Benjamin, Tamara Dinev and Robert Willison (2017), "Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda," *European Journal of Information Systems,* 26 (6), 546–63.

Lwin, May O., Andrea J.S. Stanaland and Anthony D. Miyazaki (2008), "Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness," *Journal of Retailing,* 84 (2), 205–17.

Malhotra, Naresh K., Sung S. Kim and James Agarwal (2004), "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Information Systems Research,* 15 (4), 336–55.

Martin, Kelly D. and Patrick E. Murphy (2017), "The Role of data privacy in marketing," *Journal of the Academy of Marketing Science,* 45 (2), 135–55.

Mathwick, Charla, Janet Wagner and Ramaprasad Unni (2010), "Computer-mediated customization tendency (CMCT) and the adaptive e-service experience," *Journal of Retailing,* 86 (1), 11–21.

Miltgen, Caroline L. and Dominique Peyrat-Guillard (2014), "Cultural and generational influences on privacy concerns: A qualitative study in seven European countries," *European Journal of Information Systems,* 23, 103–25.

Mothersbaugh, David L., William K. Foxx, Sharon E. Beatty and Sijun Wang (2012), "Disclosure antecedents in an online service context: The role of sensitivity of information," *Journal of Service Research,* 15 (1), 76–98.

Okazaki, Shintaro, María Ángeles Navarro-Bailón and Francisco-Jose Molina-Castillo (2012), "Privacy concerns in quick response code mobile promotion: The role of social anxiety and situational involvement," *International Journal of Electronic Commerce,* 16 (4), 91–120.

Okazaki, Shintaro, Kirk Plangger, Douglas West and Héctor D. Menéndez (2020), "Exploring digital corporate social responsibility communications on Twitter," *Journal of Business Research,*, http://dx.doi.org/10.1016/j.jbusres.2019.09.006

Orth, Ulrich R. and Roberta C. Crouch (2014), "Is Beauty in the aisles of the retailer? Package processing in visually complex contexts," *Journal of Retailing,* 90 (4), 524–37.

Palmatier, Robert W., Mark B. Houston and John Hulland (2018), "Review Articles: Purpose, Process, and Structure," *Journal of the Academy of Marketing Science,* 46 (1), 1–8.

Pan, Yue and George M. Zinkhan (2006), "Exploring the impact of online privacy disclosures on consumer trust," *Journal of Retailing,* 82 (4), 331–8.

Pavlou, Paul A. (2011), "State of the information privacy literature: Where are we now and where should we go?," *MIS Quarterly,* 35 (4), 977–88.

Peytchev, Andy, Rodney K. Baxter and Lisa R. Carley-Baxter (2009), "Not all survey effort is equal: Reduction of nonresponse bias and nonresponse error," *Public Opinion Quarterly,* 73 (4), 785–806.

Plangger, Kirk and Matteo Montecchi (2020), "Thinking beyond privacy calculus: Investigating reactions to customer surveillance," *Journal of Interactive Marketing,* 50, 32–44.

Plangger, Kirk and Richard T. Watson (2015), "Balancing customer privacy, secrets, and surveillance: Insights and management," *Business Horizons,* 58 (6), 625–33.

Rainie, Lee and Maeve Duggan (2016), *Privacy and Information Sharing,* Pew Research Center [available at http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/]

Raudenbush, Stephen W. and Anthony S. Bryk (2002), *Hierarchical Linear Models: Application and Data Analysis Methods,* Thousand Oaks, CA: Sage Publications.

Rosen, Guy (2018), *Security Update,* Facebook Newsroom [available at https://newsroom.fb.com/news/2018/09/security-update/]

Rosenthal, Robert (1979), "The 'File drawer problem' and tolerance for null results," *Psychological Bulletin,* 86 (3), 638–41.

Rubera, Gaia and Ahmet H. Kirca (2012), "Firm innovativeness and its performance outcomes: A meta-analytic review and theoretical integration," *Journal of Marketing,* 76 (3), 130–47.

Sheehan, Kim B. and Mariea G. Hoy (2000), "Dimensions of privacy concern among online consumers," *Journal of Public Policy & Marketing,* 19 (1), 62–73.

Smith, H. Jeff, Tamary Dinev and Heng Xu (2011), "Information privacy research: An interdisciplinary review," *MIS Quarterly,* 35 (4), 989–1015.

Smith, H. Jeff, Sandra J. Milberg and Sandra J. Burke (1996), "Information privacy: Measuring individuals' concerns about organizational practices," *MIS Quarterly,* 20 (2), 167–96.

Tully, Stephanie M. and Russell S. Winer (2014), "The Role of the beneficiary in willingness to pay for socially responsible products: A meta-analysis," *Journal of Retailing,* 90 (2), 255–74.

Vargas, Patrick T., Brittany R. Duff and Ronald J. Faber (2017), "A Practical guide to experimental advertising research," *Journal of Advertising,* 46 (1), 101–14.

Wang, Yanbo, Qingfei Min and Shengnan Han (2016), "Understanding the effects of trust and risk on individual behavior toward social media platforms: A meta-analysis of the empirical evidence," *Computers in Human Behavior,* 56, 34–44.

Weber, Mathias, Marc Ziegele and Anna Schnauber (2013), "Blaming the victim: The effects of extraversion and information disclosure on guilt attributions in cyberbullying," *Cyberpsychology, Behavior, and Social Networking,* 16 (4), 254–9.

Wright, Peter (1986), "Schemer schema: Consumers' intuitive theories about marketers' influence tactics," *Advances in Consumer Research,* 13, 1–3.

Whittaker, Zach (2019), *Marriott to face $123 million fine by UK authorities over data breach,* TechCrunch available online: https://tcrn.ch/2JqiGqF [Accessed January 21, 2020]

Please cite this article in press as: Okazaki, Shintaro, et al, Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review, *Journal of Retailing* (xxx, 2020), https://doi.org/10.1016/j.jretai.2020.05.007

Yun, Haejung, Gwanhoo Lee and Dan Kim (2014), "A meta-analytic review of empirical research on online information privacy concerns: Antecedents, outcomes, and moderators," *Proceedings of the International Conference on Information Systems, 35*,, 1–13.

Zhang, Jie, Paul W. Farris, John W. Irvin, Tarun Kushwaha, Thomas J. Steenburgh and Barton A. Weitz (2010), "Crafting integrated multi-channel retailing strategies," *Journal of Interactive Marketing,* 24 (2), 168–80.

Zhu, Ruilin and Youyou Tao (2015), "A ten-year longitudinal review of information privacy research from 2005–2014," in *Proceedings of the Workshop of Information Technology and Systems*, 1–15.

Please cite this article in press as: Okazaki, Shintaro, et al, Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review, *Journal of Retailing* (xxx, 2020), https://doi.org/10.1016/j.jretai.2020.05.007